2013

Combinatorial Computing-One Object Per Clock

Butler, Jon T.

Monterey, California. Naval Postgraduate School

Proc. of the Reed-Muller Workshop 2013, Toyama, Japan, May 24-25, 2013, pp. 66-79

Combinatorial Computing-One Object Per Clock

Jon T. Butler
Naval Postgraduate School,
Monterey, CA, USA

Tsutomu Sasao
Meiju University
Kawasaki, Kanagawa, JAPAN

This paper is on pp. 66-74 of the proceedings.

Combinatorial Objects Include

1. Combinations
2. Permutations
3. Partitions
4. Prime numbers
5. Palindromes
6. Binary tuples w/ even 1's
7. Bent functions

...and many others.

1

Motivation

Bent functions, useful in encryption applications, can be generated by a **sieve** process on a reconfigurable computer that is 60,000x faster than on a conventional computer.

Schafer et al - FCCM 2010

2

Motivation

However, there is **no** known method to **generate** bent functions at one per clock using a simple circuit.

Therefore, in spite of the 60,000x speedup, producing bent functions is a **very slow process.**

3

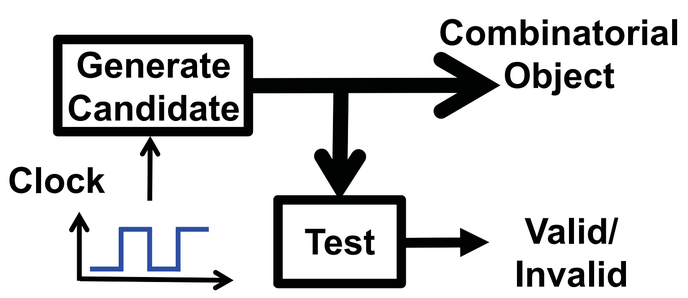
Can we Generate Bent Functions at One Per Clock?

Theorem: For every sieving circuit, there is a direct enumeration circuit that produces the same set of objects at one object per clock. ***YES!***

*However, the direct enumeration circuit may have **exponential** complexity !*

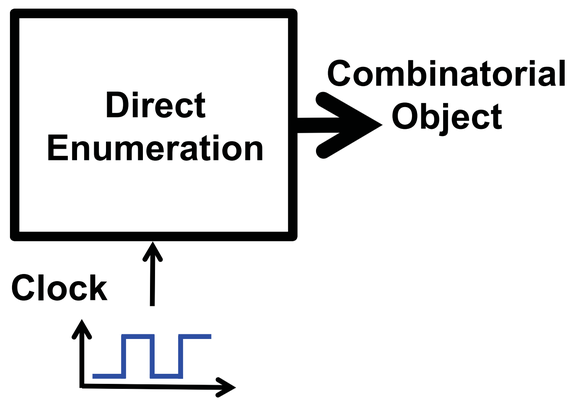
4

Sieving



5

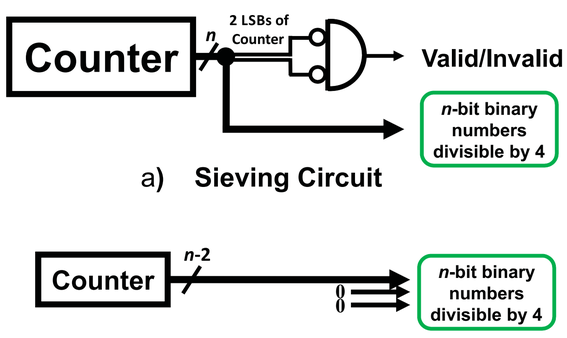
Direct Enumeration



6

Divide by 4 Circuit

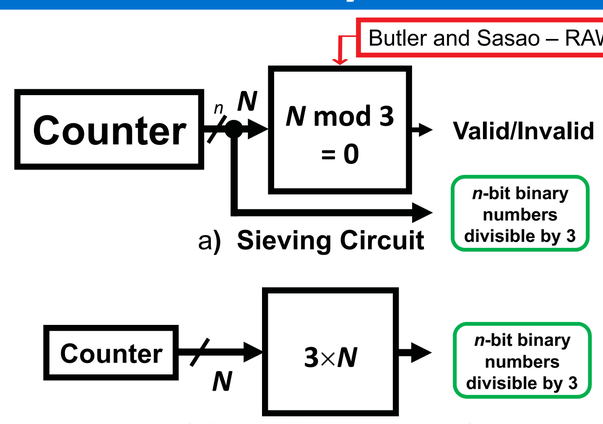
SIMPLE



b) Direct Enumeration Circuit

7

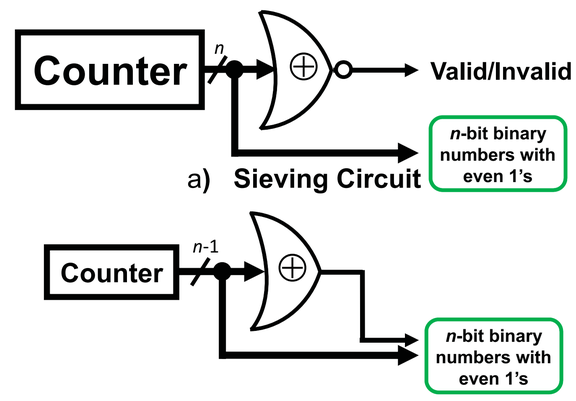
Divide by 3 Circuit



b) Direct Enumeration Circuit

8

Even 1's Circuit

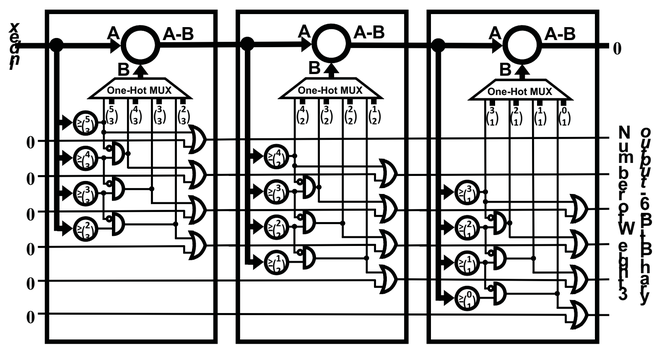


b) Direct Enumeration Circuit

9

Combination Generator

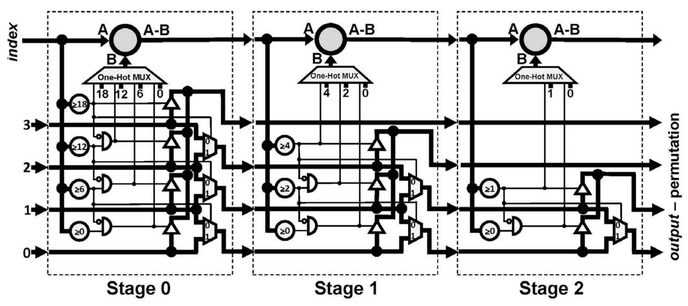
COMPLEX



Butler and Sasao – ARC 2011

10

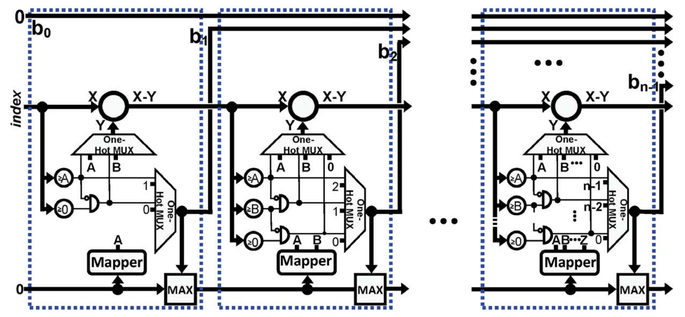
Permutation Generator



Butler and Sasao – RAW 2012

11

Set Partition Generator



Butler and Sasao – ARC 2013

12

Solved Questions

Fundamental Question
What combinational objects can be easily computed at one per clock?

1) Set partitions
2) Combinations — YES
3) Permutations

... plus many others

13

Open Questions

Some combinational objects seem to be difficult (perhaps impossible) to generate at one per clock by a **simple** circuit. However, one can sieve for them using simple circuits.

1) Bent Boolean functions
2) Monotone Boolean functions — ?

14

Contributions

We showed that combinatorial objects that can be sieved can also be directly enumerated (by circuits that may have exponential complexity).

Interesting objects whose direct enumeration circuits seem exponential include:

1) Bent functions and
2) Monotone functions.

15